Integrating Grafana and Check_MK

TruePath Technologies
Who Is TruePath Technologies Inc.

Premiere Check_MK Partner in North and South America that specializes in sales, support and managed services. Since 2006, TruePath has provided industry-leading monitoring software, hardware, and services that put you, the customer, first.

We specialize in configuring and maintaining your monitoring software so you can avoid costly network downtime and maintenance and focus on what’s most important: moving your business forward.

Douglas Mauro is the Founder and Senior Engineer at TruePath Technologies Inc. with over 20 years of experience in enterprise data centers. He's an O'Reilly author of Amazon’s #1 selling network management book "Essential SNMP" (now in it's second edition).

Email: dmauro@truepathtechnologies.com
LinkedIn: www.linkedin.com/in/douglasmauro
Phone: 585-672-5481
Cell: 716-474-1641
What Is Grafana?

- Web-based graphing engine
- Compose interactive dashboards
- Open source (GoLang)
Why Do We Want Grafana?

- Rich visualizations
- Correlate data across sources
- Extensible

Officially Supported Data-Sources:

- Graphite
- Prometheus
- InfluxDB
- Elasticsearch
- Google Stackdriver
- AWS CloudWatch
- Azure Monitor
- Loki
- MySQL
- PostgreSQL
- Microsoft SQL Server (MSSQL)
- OpenTSDB
- Testdata

https://grafana.com/plugins
Architecture

How do we build this?
Two Methods

Directly via the NEW Grafana datasource

Graphite Export to InfluxDB
Common Topologies

Depending on scale and use-case, there are many ways to deploy.
InfluxDB

- High performance time-series database
- Natively supports the Graphite protocol
- Efficient storage
- Open source (GoLang)
InfluxDB System Requirements

<table>
<thead>
<tr>
<th>Load</th>
<th>Writes Per Second</th>
<th>Queries Per Second</th>
<th>Unique Series</th>
<th>CPU</th>
<th>RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>&lt; 5 Thousand</td>
<td>&lt; 5</td>
<td>&lt; 100 thousand</td>
<td>2-4 Cores</td>
<td>2-4 GB</td>
</tr>
<tr>
<td>Med</td>
<td>&lt; 250 Thousand</td>
<td>&lt; 25</td>
<td>&lt; 1 million</td>
<td>4-6 Cores</td>
<td>8-32 GB</td>
</tr>
<tr>
<td>High</td>
<td>&gt; 250 Thousand</td>
<td>&gt; 25</td>
<td>&gt; 1 million</td>
<td>8 + Cores</td>
<td>32 + GB</td>
</tr>
</tbody>
</table>

https://docs.influxdata.com/influxdb/v1.7/guides/hardware_sizing/

Open source edition does NOT support clustering / high availability
InfluxDB Installation

1. Install the package
   Stand-alone or as added repository.
   https://docs.influxdata.com/influxdb/v1.7/introduction/installation/

2. Configure the Graphite endpoint ( /etc/influxdb/influxdb.conf )
   ```
   [[graphite]]
   # Determines whether the graphite endpoint is enabled.
   enabled = true
   database = "check_mk"
   ```

3. Start the InfluxDB service
Check_MK Configuration

- Graphite export is supported by Check_MK Enterprise Edition

  Performance data is split at the Micro Core when a check completes.
  The data is pushed to the Graphite endpoint in real-time.
  If the endpoint can not be contacted, the data is discarded.
Check_MK Configuration

Global Settings > Monitoring Core

SEND METRICS TO GRAPHITE / INFLUXDB

Current setting

Hostname / IP address of Graphite server
127.0.0.1

TCP port of Carbon line receiver
2003

Optional variable prefix:

C-style name mangling

Add new Graphite / InfluxDB connection

Factory setting

No connections defined

Current state

Hostname / IP address of Graphite server: 127.0.0.1
TCP port of Carbon line receiver: 2003
Optional variable prefix:
C-style name mangling: off

More configuration available in Host & Service Parameters

SEND METRICS TO GRAPHITE / INFLUXDB

Value
- Unit of measurement
- Warning threshold
- Critical threshold
- Minimum
- Maximum
Check_MK Configuration

Check_MK does not proxy the metrics through the master.

Each site must be able to directly contact the Influx server.

If using a single Influx server behind a firewall or on a separate network, a VPN could be used to allow this contact.

A more advanced case would be running influx in a HA configuration with endpoints in each network.
Check_MK Configuration

After changes are activated, we should start seeing metrics in InfluxDB.

> show series
key
---
Laptop.CPU_load.load1
Laptop.CPU_load.load15
Laptop.CPU_load.load5
Laptop.CPU_utilization.guest
Laptop.CPU_utilization.steal
Laptop.CPU_utilization.system
Laptop.CPU_utilization.user
Laptop.CPU_utilization.wait
Laptop.Check_MK.children_system_time
Laptop.Check_MK.children_user_time
Laptop.Check_MK.cmk_time_agent
Laptop.Check_MK.execution_time
Laptop.Check_MK.system_time
Laptop.Check_MK.user_time
...etc

> show databases;
name: databases
name
----
_internal
check_mk

> use check_mk
Using database check_mk
Grafana Installation

1. Install the package
   Stand-alone or as added repository.
   http://docs.grafana.org/installation/

2. Start the grafana-server service
   (The Grafana configuration file is /etc/grafana/grafana.ini)
Grafana Configuration

- Binds to port 3000 by default
  - There are multiple ways to handle a port change depending on topology.
  - In the instance of a dedicated grafana server where port 80 is not already in use
  - Grafana needs “Linux capabilities” set in order to bind a well-known port.
  - A reverse proxy to the default port 3000 may be used in the instance that a web server is already present.

http://docs.grafana.org/installation/configuration/#http-port
Grafana Configuration

- Database Provider

  By default Grafana uses an sqlite3 database to store its configuration.

  Two other back-ends are supported: MySQL/MariaDB and PostgreSQL.

  Either MySQL/MariaDB or PostgreSQL must be used to allow HA/Containerization.

  Consider the cost of disk operations when using the sqlite3 database.
Overview

How do we see Check_MK Data in Grafana?
How Check_MK Formats Data

Check_MK concatenates the host and service name and uses this name to create a series.

Each series contains a key named “value” with last measurement.

Check_MK does NOT currently make use of tagging available in InfluxDB

```bash
> show series
key
---
Laptop.CPU_load.load1
Laptop.CPU_load.load15
Laptop.CPU_load.load5
Laptop.CPU_utilization.guest
Laptop.CPU_utilization.steal
Laptop.CPU_utilization.system
Laptop.CPU_utilization.user
Laptop.CPU_utilization.wait
Laptop.Check_MK.children_system_time
Laptop.Check_MK.children_user_time
Laptop.Check_MK.cmk_time_agent
Laptop.Check_MK.execution_time
Laptop.Check_MK.system_time
Laptop.Check_MK.user_time
...etc
```
Adding A Datasource

A data source is a connector to a storage back-end, such as InfluxDB.

Each data source has a query editor that is customized for the specific back-end.

Data sources can return either a Time-Series or a Table.
Creating a Basic Graph

Each dashboard widget consists of one or more queries to a datasource.

Each widget can only query one source at a time and may not be mixed.
Variables

Grafana supports creation of custom variables in dashboards.

Variables can be as simple or complex as needed.

They allow for creation of dashboard templates.

http://docs.grafana.org/reference/templating/#variable-types
Variables

Variables are interpolated in the query and are passable via the URL.

http://grafanaserver/d/HdGBxKqmz/cpu-utilization?orgId=1&var-hostname=monitor01

Using these custom URLs we can dynamically link hosts and services from the Check_MK UI.
Add Actions To Check_MK

CUSTOM ICONS AND ACTIONS

Current setting

ID: CMongo

Icon:

Title: CMongo

Action:


Open in:

Show in column:
- Directly show the action icon in the column
- Sort index

Add new element

Factory setting:
0 icons and actions

Current state:
1 icon and actions

STATE HOST ICONS OK WA UN CR PD
UP Monitor01 ☀ 25 0 0 0 0
Add Actions To Check_MK

Of course, these actions are rule based!
We can customize variables in the URL for different types of hosts.
Combining Data Sources
Combining Data Sources

- Aggregation from multiple sources allows a Look into the system from many angles at once or a deep dive into a specific metric.

By leveraging variables in Grafana, and Check_MK's rule based action icons, we can build one-click access to collections of device or environment specific data that can aid in the diagnosis of issues or provide business insights.
ntopng offers real time traffic monitoring with DPI.

Integration with Grafana allows us to graph network traffic in an interesting way.

For example, if high traffic volume occurs on a device or a network segment, we are able to see a protocol breakdown immediately.
Account Management / Multi-User

- Grafana is not just for administrators!
- In addition to the built-in SQL database, Grafana supports several authentication methods suitable for large deployments.

  LDAP
  Reverse Proxy
  O-Auth Integrations

http://docs.grafana.org/auth/overview/
Account Management / Multi-User

Grafana allows for easy account management by dividing users into organizations and teams.

For instance, if you were an ISP such as a VPS company, it would be possible to provide customer portals with access to metrics, billing, or even support information.
Account Management / Multi-User

- End users don’t usually need access to the monitor.
  
  Users are typically read only and in charge of a small number of systems or operations. This also reduces load of the monitor with large user base.

- Easily Automate

  Grafana clearly exposes its HTTP API for use in automation. It is very easy to deploy and manage dashboards for users and organizations.

  [http://docs.grafana.org/http_api/](http://docs.grafana.org/http_api/)
Further Customization

Widgets, Visualizations and Features
As Interactive as you like
As Interactive as you like
Thank You!

https://grafana.com/grafana/testimonials

https://truepathttechnologies.com/check_mk/

Questions & Answers